EXHIBIT B

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION
No. 5:18-CR-00461-B0

Defense Information Systems Agency Victim Impact Statement

I, Fred P. Ruonavar, am the Chief of the DISA Mission Division. I have been the Chief of the DISA Mission Division for nine years. Through my current position, I am responsible for analyzing the different contingency and operation's plans and assessing the requirements of the Command, Control, Communications, Computers, and Intelligence (C4I) systems supporting Department of Defense (DoD) military operations globally.

The Defense Information Systems Agency has a wide portfolio of responsibilities, including providing internet access points to Department of Defense organizations. DISA monitors DoD internet traffic and works with our commercial internet provider partners to analyze and defend the DoD information network. We have our own internal monitoring and defense systems and pay our commercial internet providers to perform their own monitoring of the traffic directed to the DoD. These efforts cost the taxpayers millions of dollars.

We are constantly under attack by malicious individuals from different backgrounds. We continually have to spend time and effort to adjust to the changing threats we face. Even though we provide some of the best information technology services in the world, the DoD networks are not invulnerable. A clever attack that successfully evades or overpowers our defense can have serious real world consequences ranging from loss of personal information belonging to our service members to crashing critical sites that provide vital logistics systems and communications to our ships, installations, or other DoD entities.

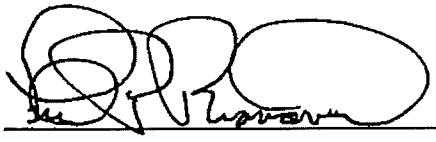
Over the course of the last 20 years, the growth of technology and the advances in computing power has proven to be a force enabler and multiplier. Our networks support DoD activities ranging from the Defense Health Agency to the command and control of unmanned aerial systems. A successful attack on our systems could result in mission failure and cost the lives of our service members. If a successful attack occurs, our leaders' ability to maintain awareness of current events and successfully control our own forces could be severely degraded. Our own forces may not even be able to communicate with each other.

Distributed denial of service (DDOS) attacks are serious threats to commercial and government networks, including the DoD networks. This is a brute force attack, in which a large quantity of traffic is sent in order to overwhelm the victim's network, server, or application resources. DDOS attacks are used by foreign governments, adversary non-nation state terrorists, "hacktivists," and cyber criminals. Over time, defenses have improved, but so have the techniques used to attack networks.

These DDOS attacks attempt to consume the victim's resources with spoofed traffic so that they are unable to process legitimate traffic. It is as if numerous protesters blocked a store's entry door, preventing customers from getting in. When a server is overloaded with connections, new connections can no longer be accepted. The attacks generated by Mr. Usatyuk included attacks against DISA itself, the Army, the Navy, the Air Force, the Pentagon and other unspecified Defense organizations.

The attacks launched by Mr. Usatyuk were serious threats DISA had to defend against. Our efforts to deal with his crimes have consumed DoD resources that would have been better used to defend the nation against our peer and near-peer competitors.

I swear under penalty of perjury that the above statement is true and correct to the best of my knowledge.



FRED P. RUONAVAR

7/29/2019